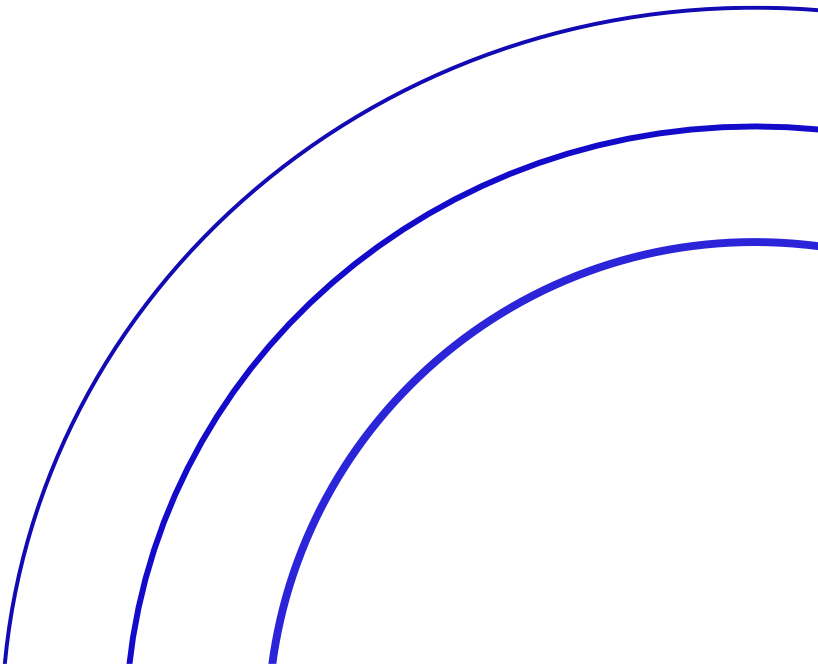
CloudDesk Service Description



Document Control

TITLE:	**CloudDesk Service Description**	**DOCUMENT REF NO:**	QMS REC53
DESCRIPTION:	This document defines the services provided by Calligo's CloudDesk service		
OWNER/ AUTHORITY:	VP, Cloud Operations	**VERSION NO:**	1.9
DOCUMENT CROSS REFERENCE:	N/A	**VERSION DATE:**	20/02/2023
DISTRIBUTION METHOD	Email and Website	**DOCUMENT CLASSIFICATION**	Internal

DOCUMENT OWNER & APPROVAL
The VP Cloud Operations is the owner of this document and is responsible for ensuring that this service description is reviewed in line with the review requirements of Calligo's Information Security Management System, Project Management Frameworks as well as the guidance and requirements of the CSSF.
Approved by the Chief Operating Officer, Calligo ("Entity") on 25 November 2022

CHANGE HISTORY RECORD				
VERSION	**DESCRIPTION OF CHANGE**	**AUTHOR**	**APPROVAL**	**DATE OF ISSUE**
1.0	Initial Issue	Director, Product & Service Development	CEO	19/10/17
1.1	Verbiage Review	Director, Product & Service Development	CEO	08/11/17
1.2	Added RACI Matrix, Glossary of Terms and amendments	Director, Product & Service Development	CEO	01/12/17
1.3	Verbiage Review	Director, Product & Service Development	Chief Experience Officer	06/01/18
1.4	Group Review	Legal Counsel	CISO	05/05/18
1.5	Verbiage Review	Legal Counsel	Director, Product & Service Development	09/08/19
1.6	Re-design, change of ownership and verbiage review	VP, Cloud Operations	Chief Operating Officer	25/11/22
1.7	Remove Service Locations table and add link to external Service Locations document.	Director, Operations Management	Chief Operating Officer	10/01/23
1.8	Updated formatting	Director, Operations Management	Chief Operating Officer	21/01/23
1.9	Updating links for supporting documentation	VP, Cloud Operations	Chief Operating Officer	20/02/23

1. Service Overview

This document defines the services provided by Calligo's CloudDesk service. The CloudDesk service is one of a suite of services within the Calligo Operating Model.

CloudDesk is a service that enables users to access a secure Virtual Desktop without having to worry about the management of the associated technologies. The service offers all the common features of an owned infrastructure without the overhead of management.

2. Service Inclusions

2.1. CO-DAAS-BDE

This service provides a service that enables users to access a secure Virtual Desktop without having to worry about the management of the associated technologies. The service offers all the common features of an owned infrastructure without the overhead of management

2.2. CO-ITSM-OSP

This service leverages Datto RMM and PowerBI to deliver patching and reporting to Windows OS assets.

2.3. CO-ITSM-SD

This service leverages an ITSM platform and trained Level 1 Service Desk Analysts to cover activities that provide a client facing Service Desk

2.4. CO-SW-LICENSE

This service provides Application, OS, and Appliance licensing.

2.5. CO-CP-SCC

This service adds Antivirus and Malware protection to the CloudCore environment.

2.6. CO-CP-MFA

This service leverages native or third-party MFA solutions

3. Service Provisions

3.1. CO-DAAS-BDE

3.1.1. Inclusions

CO-DAAS-BDE	
Scope Item	**Description**
IaaS environment	This element of service is described in **SI: CO-CC-BVDC**
Virtual Desktop Templates	Configuration and management of virtual desktop template deployed in the provision of the CloudDesk service
Application Support	Configuration and management of standard applications deployed in the provision of the CloudDesk service
Licensing	This element of service is described in **SI: CO-SW-LICENSE**
Anti-Malware	This element of service is described in **SI: CO-CP-SCC**

Gold Image	Configuration & management of master image (Gold Build) template virtual desktops
User profiles Management	Creation and management of user profiles and persona storage
Patching	This element of service is described in **SI: CO-ITSM-OSP**
Desktop support	Troubleshooting virtual desktop issues
MFA	This element of service is described in **SI: CO-CP-MFA**
Access Management	Configuration and management of Role based Access Control Policy (RBAC) based on client specifications

3.1.2. Exclusions

CO-DAAS-BDE	
Exclusion Item	**Description**
CloudDesk Specification	Specification of client CloudDesk systems (e.g.: specification of virtual desktop size, quantity, desktop pools)
Application Support	Configuration and management of client virtual desktop applications Logging and monitoring of client environment and applications Rectifying user issues with Third-Party Applications or Third-Party Services
Licensing	Add on as required (Additional Cost) - This element of service is described in SI: **CO-SW-LICENSE**
Service connections	Maintain compatible physical client devices to connect to the service
Physical devices	Troubleshooting of issues with physical client devices
SOC	Security operation management (SOC) of client environment

3.2. CO-ITSM-MON

3.2.1. Inclusions

CO-ITSM-MON	
Scope Item	**Description**
Base OS Monitoring	Monitoring covers in-support Windows Server family operating systems
Resource Monitoring	The following items are currently within scope -CPU utilization -Memory (RAM) utilization -Disk utilization
Availability Monitoring	-RMM Agent heartbeat -URL availability
Remediation	-Remediation services to ensure all management functionality is operable -Remediation services to restore operability, or resolve service availability issues of monitored options
Service Monitoring	Monitoring of core OS and role services (defined as per service design)

3.2.2. Exclusions

CO-ITSM-MON	
Exclusion Item	**Description**
End-of-Life OS	Microsoft OS that has passed end of support date and no extended support agreement exists
End user OS	Non-Windows Server OSes (e.g., Windows 10)
Non-OS application	3rd party software installed to a monitored system Troubleshooting of issues at the application level for applications related to services not provided by Calligo.
Licensing	Application or Server licensing expiration or renewal periods

Customer Internet Connectivity	Monitoring of external IP addresses for connectivity
Procurement	As part of remediation activities, procurement of required hardware or software is out of scope and requires a separate service agreement
Specific Functionality	Monitoring can detect if a system or service is available, but cannot validate full functionality

3.3. CO-ITSM-OSP

3.3.1. Inclusions

CO-ITSM-OSP	
Scope Item	**Description**
Monthly patching of systems running Windows OS currently supported by Microsoft	For supported OS versions: Deprecated OS versions require a separate Microsoft Extended Support Contract and a separate deployment agreement. Applicable patches are automatically approved unless otherwise agreed via Patch Advisory reporting and additional approval workflows. Critical, Monthly and Security updates are included as part of regular patch deployments.
Configuration and maintenance of deployment rules, settings, and deployment options.	Administration of rules, products, update classifications, agent settings Zero-day patch deployment
Consolidation of Monthly updates into cumulative updates and deployment of the cumulative updates.	Previous months applicable patches are consolidated into a single deployment to cover all patches in all previous deployments. These deployments are active with the current months deployments and follow the same schedule.
Maintenance of groups for systems in scope	Checking health and heartbeat of assigned assets in specific groups and schedules.
Exclusion of patches from deployment scope for known issues with the patch or resulting from testing during the pilot deployment	Removal of patches from deployment scope for known issues with the patch or as a result of testing during the pilot deployment.
Standard Reporting	Standard Monthly and regularly scheduled reports are included in this service.

3.3.2. Exclusions

CO-ITSM-OSP	
Exclusion Item	**Description**
The development of patch “work arounds” in the absence of an approved system vendor’s patch.	This is a chargeable addition to the service and is priced on effort required as each mitigation or “work around” is unique.
Ad-hoc and /or custom patch reporting	This is a chargeable addition to the service and is priced on effort required.
Manual Patching of systems	This is a chargeable addition to the service and is priced on effort required.
Removal of patches from systems once installed	This is a chargeable addition to the service and is priced on effort required as backouts can vary and be unique.
Remediation or recovery of non-compliant systems caused due to existing OS issue.	The required patches are identified, downloaded and the installation is attempted but fails due to OS issues. Any troubleshooting beyond included remediation steps is a chargeable addition to the service. If the server blue screens due to applied patches during or immediately after patch installation, any troubleshooting beyond included remediation steps is a chargeable addition to the service.
Performing manual vulnerability remediation steps.	Manual steps required before or after automated patching windows is a chargeable addition to the service and is priced on effort required. This falls into the same area as “Manual patching of systems” above.
Compliance on assets added/removed without notification, or where	Calligo needs to be informed in the form of a change record to the scope or configuration changes that could impact agent's health and the patching process.

configuration changes have been made to assets without submission via Change Management Process	

3.4. CO-ITSM-SD

3.4.1. Inclusions

CO-ITSM-SD	
Scope Item	**Description**
Access to the Calligo ITSM platform	24/7 access to the Calligo ITSM platform that provides capabilities for clients to raise new support tickets and to access open or historic support tickets.
Telephone Support	Access to the Calligo Service Desk via the issued telephone contact numbers during regional Business Hours only.
First Line Fix	Access to the Calligo L1 Service Desk Analysts for first line fix or resolution.

3.4.2. Exclusions

CO-ITSM-SD	
Exclusion Item	**Description**
24/7 Telephone Support	This is a chargeable addition.
Onsite support	All support delivered via the Service Desk offering is remote.

3.5. CO-SW-LICENSE

3.5.1 Inclusions

CO-SW-LICENCE	
Scope Item	**Description**
Client Agreement	Creation of a Customer Agreement, between the client and Application, or OS Vendor
Manage licenses	Management of products and service subscription licenses
Billing Support	Provide billing support from application or OS vendor
Manage Tenant Subscription	Managed subscription changes on behalf of the Client
Reporting	Provide license total / usage
Invoicing	Invoice creation and delivery

3.5.2 Exclusions

CO-SW-LICENCE	
Exclusion Item	**Description**
Installation of software	This element of service is described in SI: **CO-ITSM-SD**
Tracking of client licensing compliance	Client is responsible for maintaining licensing compliance on applications and OS

3.6. CO-CP-SCC

3.6.1 Inclusions

CO-CP-SW	
Scope Item	**Description**

Installation of Anti-Malware	Anti-malware protection tooling for applicable CloudCore servers
Configuration of Protection Policy	Best practice scan rules applied as default
Notification of detection of malware or virus	Report generation of an outbreak

3.6.2 Exclusions

CO-CP-SW	
Exclusion Item	**Description**
End-of-Life OS	Microsoft OSs that are no longer supported by current tooling.
Non-Windows OS	Calligo does not support Unix, Linux, iOS for Antimalware scanning?
Remediation activities because of a virus or malware outbreak	Client is responsible for any remediation activities required to its own- or third-party applications, Data and services.

3.7. CO-CP-MFA

3.7.1. Inclusions

CO-CP-MFA	
Scope Item	**Description**
Enrolment	New device or user enrolment
Application integration	Integrate Calligo-supplied MFA with natively supported applications
Remediation of MFA services issues	Remediation of systemic system issues

3.7.2. Exclusions

CO-CP-MFA	
Exclusion Item	**Description**
Client network connectivity	An active internet connection is required on the mobile device to receive MFA push notifications
Custom application integration	Custom applications developed by the customer or contracted organization
End user device	Device issues unrelated to MFA
Credentials	First-factor authentication (e.g., password) issues

4. Roles and Responsibilities

The table below provides a responsibility matrix for the core CloudDesk elements:

Service Activities – Core Elements	Calligo	Customer
CO-DAAS-BDE		
Configuration and management of virtual desktop template deployed in the provision of the Service	R, A	
Configuration and management of supported applications deployed in the provision of the Service	R, A	
Licensing of virtual desktop Operating System & Microsoft applications deployed in the provision of the Service	R, A	
Specification of Client DaaS systems (e.g.: specification of virtual desktop size, quantity, desktop pools)	C	R, A

Configuration & management of master image (Gold Build) template virtual desktops	R, A	C
Specification of network and firewall configuration	C, I	R, A
Configuration of network and firewalls based on Client specification	R, A	C
Creation and management of user profiles and persona storage	R, A	C
Datacenter internet connectivity	R, A	I
Client internet connectivity	I	R, A
Licensing of Client virtual desktops and Operating Systems	R, A	
Licensing of Client virtual desktop Microsoft applications	R*, I*	R, A
Licensing of Client virtual desktop non-Microsoft applications	I	R, A
Maintain a compatible physical Client device to connect to the service[1]	C	R, A
Troubleshooting of issues with physical connection devices	R	A, C
Troubleshooting virtual desktop issues relating to supporting infrastructure and operating system	R, A	C
Logging and monitoring of Client environment and applications		R, A
Patching client Virtual Machine Operating System & applications	R, A	C
Testing of client Virtual Machine Operating Systems patches applied	C	R, A
Configuration and monitoring of Antivirus/Malware protection for Virtual Machine	R, A	C, I
Specification of Role Based Access Control (RBAC) Policy	C, I	R, A
Configuration and management of RBAC	R, A	C, I
Troubleshooting of user issues with the Virtual Machine	R, A	
Rectifying user issues with Third-Party Applications or Third-Party Services	C	R, A
Rectify User issues with Virtual Machine	R, A	I
Management of Virtual Machine Public IP addresses	R, A	C
Monitoring and management of IP bandwidth	R, A	I
CO-ITSM-OSP		
Business application verification, maintenance, and testing	C, I	R, A
Patch Deployment	R, A, C	
Defining standard recurring deployment schedules, exclusions, and targets	C, I	R, A
Compliance measurement for SLO/SLA purposes	R, A, C	I
Maintenance of SCEM collections for systems in scope	R, A, C	I
Add and remove systems to scope	R, A	C, I
Review released list of patches from Microsoft and provide customer notification prior to scheduled installation	R, A	C, I
Identify patches to be excluded and approve list of patches for deployment	C, I	R, A
Identify business areas that require patch reporting and provide contact information for recipients	C, I	R, A
Provide SMTP relay for subscription-based delivery of reports and alerts	C, I	R, A
Run reports on a scheduled basis and provide malware detection alerts	R, A	C, I
Identify patches to be excluded and approve list of patches for deployment	C, I	R, A
Identify business areas that require patch reporting and provide contact information for recipients	C, I	R, A
Provide SMTP relay for subscription-based delivery of reports and alerts	C, I	R, A
Run reports on a scheduled basis and provide malware detection alerts	R, A	C, I
CO-ITSM-MON		
Configuring standard monitoring	R, A	C, I
Requesting monitoring changes	R, C	R, A

[1] Please refer to the list of compatible devices on the Calligo website

Responding to alerts	R, A	C, I
Remediation	R	R, I
CO-ITSM-SD		
Raising support requests	R	R, A
Contacting Calligo Service Desk via telephone for P1 Support Requests	I	R, A
Correctly assigned the right category and priority to all incoming support requests	R, A	C, I
Providing full and detailed information when creating new support requests	I	R, A
Providing detailed and regular ticket updates	R, A	I
Responding to all ticket updates where additional information or testing is requested from Calligo Service Desk	I	R, A
Providing prompt confirmation of ticket closure agreements.	I	R, A
CO-SW-LICENCE		
Create a valid Customer Agreement between Application or OS vendor and Client	R, A	I
Accurate count of licenses required	A	R
Request changes to subscription being managed	I	R, A
Provide subscription billing invoices for managed subscriptions	A, R	I
Payment of subscription invoices from Calligo	I	R, A
CO-CP-SCC		
Monitoring and management of the Anti-Malware infrastructure	R, A	
Ensuring Anti-Malware is in place for all protected endpoints in scope	R, A	I
Ensuring that default policies are pushed to all endpoints in scope	R, A	
Ensuring that the Anti-Malware definitions are updated within 48hrs of release	R, A	I
Notification of a virus or malware outbreak event	R, A	I
Infection remediation activities as defined in remediation runbook	R, A	I
Specific client data and application remediation activities as a result of a virus or malware outbreak	I, C	R, A
CO-CP-MFA		
Enrolment of new users and new devices	R, A	R, A
Unlocking accounts	R, A	C
Account lockout	R, A	R
Application Integration	R, A, C	C, I
Remediation of systemic issue	R. A	C, I

* Subject to having purchased Microsoft SPLA licensing from Calligo

R=Responsible, A=Accountable, C=Consulted, I=Informed

5. Reporting

The table below provides details on the additional Monthly Reporting and Analytics for CloudDesk that are included in the core service:

Service Item	Reporting Item	Description	Frequency
CO-ITSM-MON	**Monitoring Performance**	Average values of resource utilization for monitored systems during the previous period	Monthly
CO-ITSM-MON	**Monitoring Alerts**	Alerts raised during the previous period and current status (open or resolved)	Monthly
CO-ITSM-MON	**Device Monitor status**	List of configured monitors for each supported system	Monthly
CO-ITSM-OSP	**Asset lists (Deployment Collections)**	List of all assets currently in scope as well as their current collection memberships and deployment windows	1 Monthly. Sent a day after Patch Tuesday

CO-ITSM-OSP	**Patch Advisory**	The report lists all required patches that are scheduled for deployment.	1 Monthly. Sent a day after Patch Tuesday
CO-ITSM-OSP	**Pre-Patch Compliance Report**	The report includes compliance summary and a list of non-compliant systems.	1 per deployment. Sent prior to deployment.
CO-ITSM-OSP	**Asset Compliance State (Current Cycle)**	Current patch compliance state for the current month deployments.	1 Monthly after deployment completion
CO-ITSM-OSP	**Asset Compliance State (Cumulative Cycle)**	Current patch compliance state for the cumulative (OS in support Date through Current – 1) deployments.	1 Monthly after deployment completion
CO-SW-LICENSE	**License Consumption report**	Report of current license(s) purchase	1 Monthly
CO-CP-SCC	**Endpoint Protection Summary**	Endpoint status summary	Daily (Automated)
CO-CP-MFA	Authentication Log	Report detailing user activity, both successful and unsuccessful authentication attempts, locked out accounts	1 per month if requested
CO-CP-MFA	Deployment Progress	Enrolled, active, unenrolled, inactive users	1 per month if requested

6. Data Residency

Calligo Data Residency

7. Service Requirements

Service Item	Requirements Item
CO-DAAS-BDE	This service requires the following service items to be purchased as well: • CO-CC-BVDC
CO-ITSM-MON	Datto RMM Agent must be installed to all monitored assets
CO-ITSM-MON	Network connectivity and necessary access rules are required for all monitored assets
CO-ITSM-OSP	Current in support or Extended support Windows OS assets.
CO-ITSM-OSP	Deployment of Datto RMM agent and relevant firewall / access configurations for each in scope asset
CO-ITSM-OSP	An agreed and defined re-occurring maintenance window for automated patch installation and remediation activities
CO-ITSM-OSP	Reboots are permitted within the agreed maintenance windows.
CO-ITSM-OSP	Outbound internet access for monitoring and patching.
CO-ITSM-SD	Client is provided information on support access methods
CO-ITSM-SD	All Priority 1 incidents are logged, and the client must follow up with a telephone call into support.
CO-CP-MFA	Mobile device running current iOS or Android operating system, with internet connectivity (necessary to receive push notifications)
CO-CP-MFA	Client server to run MFA authentication proxy (where applicable)

8. Access Requirements

Requirements Item
Administrative access to all assets in scope as required for remediation actions
Service account for Datto RMM agent activities
Clients can access the service via any of the supported devices that the Client installed, or via a compatible web browser supporting HTML5. Details of the latest supported list can be found in the Calligo compatibility matrix (See related Documents)
The Client agrees to maintain a permanent, dedicated Internet connection with sufficient bandwidth to enable Calligo to deliver this service within agreed SLO's. Bandwidth requirements will increase with amount of data protected and change rate.
Administrative access to the MFA management interface. This is necessary to configure integrations, enrol users, and troubleshoot issues

Administrative access to server running authentication proxy. This is necessary to troubleshoot connectivity and authentication failures

Administrative access to directory server and any systems utilizing the authentication proxy. This is necessary to troubleshoot authentication failures.

9. Support Locations

Calligo Support Locations

10. Service Catalogue Request Items

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
Monitoring Report	48BHR	Provides data available from the platform	1 per week
Additional service monitoring	48BHR	Additional monitors may be added to existing systems	1 per week
Modify alert recipients	48BHR	Alert recipients may be adjusted to include client stakeholders	1 per week
Modify alert thresholds	48BHR	Client may request custom thresholds for an alert to be raised	1 per week
On demand tracking of compliance states	1BHR	Specific KB patch tracking submission	1 Monthly
VDI Resizing	1 Business Day	No previous request in the current month for the impacted VDI	10 Monthly
New VDI	1 Business Day		10 Monthly
Removal of VDI	1 Business Day		10 Monthly
New user enrolment	8BHR	Enrol a new user in MFA	5 per week
New device enrolment	8BHR	Enrol an existing user's new device	5 per week
Unlock user account	4BHR	Unlock a locked account	5 per week
Lock user account	8BHR	Prevent a user signing in	5 per week
Integrate application	24BHR	Integrate MFA with a supported application	1 per month
Reporting	24BHR	Generate MFA activity report	1 per week

11. Standard SLO's

Service-Level-Agreement.pdf (calligo.io)

12. Related Documents

Supporting documents for this service:

Calligo - Compatibility Matrix.pdf

Any clients onboarding to Calligo will require the following document as an introduction to service

Calligo – Welcome to Support for Clients

13. Optional Services

In addition to the CloudDesk service, Calligo can provide the following service items as optional add on services for CloudDesk:

Service Item	Service Item Reference	Description
Service Delivery Manager	CO-ITSM-SDM	The Service Delivery Manager will be responsible for the business as usual and account management relationship. This will include service reviews, point of escalation, responsible for Information Technology Infrastructure Library (ITIL) practice adherence, interfacing with third-party suppliers also participating under the customer's Service Integration and Management model and ensuring that Calligo meets or exceeds Service Level Objective (SLO) targets.
Technical Account Manager	CO-ITSM-TAM	The Technical Account Manager will be responsible for the technical collaboration between the customer and Calligo support teams and will play a key role in technical service improvement, managing deployment of new services or configuration changes, ensuring optimal performance and uptime of the application stack, and interfacing with third-party suppliers as required under the customer's support model.
M365 Threat Protection	CO-ITMS-M365TP	Calligo's M365 Threat protection provides endpoint level Antivirus and Malware protection.
M365 Threat Protection	CO-ITMS-M365APP	Calligo's M365 Application support provides real time monitoring of the M365 Tenant as well as User management and Mailbox provisioning. Technical support is provided for Word, Excel, PowerPoint, Teams, Outlook, OneDrive and SharePoint Online.
Application Currency	CO-ITMS-ACAAS	Calligo's Application Currency as a Service adds and additional layer of patch currency and security to installed third party applications.

14. Auxiliary Services

14.1. Service Onboarding & Transition

To launch CloudDesk service successfully, service design, onboarding and transition will be required to prepare and test both the environment and the managed services processes. Calligo will undertake several workshops to discuss and confirm each element of the service to ensure all parties are aware of roles and responsibilities in advance of service launch.

Service transition and onboarding covers areas such as ticket management setup, platform readiness with knowledge share, and finalising all ITIL practices. A test and acceptance criteria are captured and signed off, to allow for the CloudDesk service to commence.

After service launch, Calligo uses a formal service transition framework as the basis to carry out acceptance into service procedures, for new services landing into managed services. We typically engage at the initial stages of a project to ensure service operation adoption and readiness is planned and carried out correctly. This materializes as follows:

- To review designs, build and test artefacts to ensure supportability.
- Attend change review boards to gain early sight of changes by way of knowledge acquisition.
- To witness and validate designs and builds are delivered as proposed and intended.
- Complete operational into service documentation, training, and runbook enablement, which is required as part of the service hand-over.

14.2. Change Request and Change Control Process:

All infrastructure changes introducing risk to the environment will require change control which includes, but not limited to, Microsoft Security Patching, Infrastructure Upgrades, Deployments, Configuration Item status change. This can be generated from maintenance or an event such as an upgrade required on the system released by Third Party vendors, requested by the customer, or from a monthly release of security patches.

Where possible Standard Changes will be used with minimal risk, repeatable implementation steps, and prior approval from the customer in the form of an email.

An Emergency, or unplanned, change process will be raised to resolve a Priority 1 or 2 incident or to implement an emergency Security Patch. This accelerates the time to implement and resolve.

All Requests for Change will be reviewed internally, assessed internally, and authorized or rejected through Calligo ITSM tool.